



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,747	10/31/2001	Richard Paul Tarquini	10014006-1	4897

7590 08/03/2005

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER
----------

PERUNGAVOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/003,747

Applicant(s)

TARQUINI, RICHARD PAUL

Examiner

Venkatanarayanan Perungavoor

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

PD

## **DETAILED ACTION**

### ***Response to Arguments***

1. The Examiner mentions that Claim 8 and 15 are rejected under 35 USC § 102(e) to U.S. Patent 6,279,113 to Vaidya.
2. The objection to the specifications is withdrawn as the application contained blanks with reference to related applications, but are remedied by filling them in.
3. The Applicant's arguments regarding Claim 1 are not persuasive. As Vaidya discloses monitoring all seven layers of the OSI model see Col 4 Ln 28-33. And further it is commonly known in the art that the OSI model includes seven layers(Physical, Data Link, Network, Transport, Session, Presentation, Application<sup>1</sup>) which includes the present invention's monitoring of application, transport and network.
4. The Applicant's arguments regarding Claim 17 are not persuasive. As Holland does disclose a network stack containing a protocol driver, a media access control driver and an intrusion prevention system transport service provider layer see Col 5 Ln 9-21 & Col 6 Ln 62-65 & Col 4 Ln 52-58 & Fig. 5 item 121. Holland discloses the drivers(media access and protocol drivers) being stored in a memory space and further discloses an IP stack where information regarding

---

<sup>1</sup> See [http://webopedia.internet.com/quick\\_ref/OSI\\_Layers.asp](http://webopedia.internet.com/quick_ref/OSI_Layers.asp) for more details.

Art Unit: 2132

layers are stored; as stated earlier transport layer of the intrusion detection system(TCP/UDP) see Col 6 Ln 47-61.

5. And further the Examiner reminds the Applicants, *In Syntex (U.S.A.) LLC V. Apotex Inc.*, 74 USPQ2d 1823 (CA FC 2005), "Prior art reference teaches away from claimed invention if it suggests that developments flowing from its disclosures are unlikely to produce objective of invention, and what reference teaches person of ordinary skill in art is not limited to what reference specifically 'talks about' or what is specifically 'mentioned' or 'written' in reference;..."

6. For citations of 35 USC § 102(e) and 35 USC § 103(a) please consult <sup>previous</sup> ~~please~~ office action.

***Response to Amendment***

***Claim Rejections - 35 USC § 102***

7. Claim 1, 5-9, 15-16 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 62791 13 to Vaidya.
8. Regarding Claim 1 , Vaidya discloses the an intrusion detection system whereby the all the seven OSI layers are monitored; which includes the application, transport and network layer see Col 4 Line 29-31 .(see discussion above relating to arguments)

9. Regarding Claim 5, Vaidya discloses the first layer(application layer) interfacing with the file system. Vaidya discloses having an memory of profiles and this profile interfacing with application session see Col 4 Line 8-10 & Line 19-22.
10. Regarding Claim 6, Vaidya discloses the file system interfacing with the first layer which includes an database for storing repods and signature file see Col 3 Line 66- Col 4 Line 39.
11. Regarding Claim 7, Vaidya discloses the first layer(application layer) providing the third layer(network layer) the signature files see Col 3 Line 40-48.
12. Regarding Claim 8, Vaidya discloses the communication session between intrusion prevention system and database system see Col 2 Line 30-53.
13. Regarding Claim 9, Vaidya discloses the an intrusion detection system whereby the all the seven OSI layers are monitored, which includes the application, transport and network layer see Col 4 Line 29-31 . Vaidya also discloses the instructions and processor see Col 6 Line 1 1-25.
14. Claim 15 is rejected under the same rationale as Claim 8 above.

15. Regarding Claim 16, Vaidya discloses the archiving of intrusion related events in a database file system see Col 4 Line 8-18 & Col 5 Line 47-51.

***Claim Rejections - 35 USC § 103***

16. Claim 2, 3, 4, 10-13, 17-19 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6279113 to Vaidya in view of U.S. 6851061 B1 to Holland 111 et al .
17. Regarding 2, 3 and 4, Vaidya does not disclose the use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library. However, Holland et al. discloses the use of filter to monitor the network layer see Column 4 Line 52-67., further discloses the use of an audit system to monitor transport layer see Column 4 Line 31-52., and also discloses the use of dynamically linked library for interfacing with the first and second layer see Col 5 Line 61-Col 6 Line 15. It would be obvious to one having ordinary skill in the art at the time of the invention to include use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library in the invention of Vaidya in order to increase internal security and latency as taught in Holland see Col 4 Line 2-19.

18. Regarding Claim 10, 12, and 13, are rejected under the same rationale as Claim 2, 3 and 4 above.

19. Regarding Claim 11, Vaidya does not disclose the initialization of stack.

However, Holland et al. discloses the initialization see Col 4 Line 43-67. It would be obvious to one having ordinary skill in the art at the time of the invention to include initialization of stack in the invention of Vaidya in order to have a clean stack for data to be put upon.

20. Regarding Claim 17, Vaidya discloses a processor, memory module see

Column 6 Line 1-26 & Col 5 Line 47-67, but does not disclose the use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library. However, Holland et al. discloses the use of filter to monitor the network layer see Column 4 Line 52-67, further discloses the use of an audit system to monitor transport layer see Column 4 Line 31-52, and also discloses the use of dynamically linked library for interfacing with the first and second layer see Col 5 Line 61-Col 6 Line 15. It would be obvious to one having ordinary skill in the art at the time of the invention to include use of drivers to monitor network layer, transport layer interface and first layer interfacing with the second layer by a dynamically linked library in the invention of Vaidya in order to increase internal security and latency as taught in Holland see Col 4 Line 2-19. (see discussion above relating to arguments)

21. Regarding Claim 18, Vaidya discloses the intrusion protection system communicating with the file system see Col 5 Line 27-33.

22. Regarding Claim 19, Vaidya discloses the logging of intrusion-related data in database for future reference see Col 5 Line 47-50.

***Conclusion***

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on



Art Unit: 2132

8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor  
Examiner  
Art Unit 2132

*VP*  
7/28/2005

*Gilberto Barron Jr.*  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100